REMARKS

Claims 107-147 and 165-181 are pending in the application.

Claims 107-147 and 165-181 have been rejected.

Claims 107, 120, 131, 140, 165, 174, 176, 178-179 and 181 have been amended.

Rejection of Claims Under 35 U.S.C. §103

Claims 107-115, 131-139, and 165-173 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,064,671 issued to Killian ("Killian") in view of U.S. Patent No. 6,643,701 issued to Aziz et al. ("Aziz").

Claims 116-119 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,064,671 issued to Killian ("Killian") in view of U.S. Patent No. 6,643,701 issued to Aziz et al. ("Aziz"), in further view of U.S. Patent No. 6,104,716 issued to Crichton et al. ("Crichton").

While not conceding that the cited references qualify as prior art, but instead to expedite prosecution, Applicants have chosen to respectfully disagree and traverse the rejection as follows. Applicants reserve the right, for example, in a continuing application, to establish that the cited references, or other references cited now or hereafter, do not qualify as prior art as to an invention embodiment previously, currently, or subsequently claimed.

In order for a claim to be rendered invalid under 35 U.S.C. § 103, the subject matter of the claim as a whole would have to be obvious to a person of ordinary skill in the art at the time the invention was made. *See* 35 U.S.C. § 103(a). This requires: (1) the reference(s) must teach or suggest all of the claim limitations; (2) there must be some teaching, suggestion or motivation to combine references either in the references themselves or in the knowledge of the art; and (3) there must be a reasonable expectation of success. *See* MPEP 2143; MPEP 2143.03; *In re Rouffet*, 149 F.3d 1350, 1355-56 (Fed. Cir. 1998).

In this regard, independent claim 107, as amended, now recites:

> 107. A method comprising:
> providing a plurality of sockets, wherein
> each socket has an associated connection and an associated security token, and
> the associated security token is provided by the associated connection;
> receiving a first connection and a first security token;
> creating a socket associated with the first connection, wherein
> the creating comprises associating the first security token with the first connection;
> comparing the first security token with the associated security tokens;
> in response to said comparing, if none of the associated security tokens match the first security token, including the socket in the plurality of sockets.

As will be appreciated, amended independent claims 120, 131, 140, 165 and 174 recite, at least in part, substantially comparable limitations.

By contrast to the foregoing, Killian, which is concerned with a multi-homed end system for increasing computers' network bandwidth, discloses:

> "Network computers have a plurality of network-level interfaces associated with overlapping portions of the network-level address space, such as those represented by multiple static entries with the same address range, or multiple default entries in a network-level routing table. The computers distribute outgoing messages address [*sic*] to the overlapping portions of the address space between the multiple network interfaces associated with those overlapping portions. In the TCP/IP environment, the distribution of messages can be performed on the basis of the outgoing message's source port, the amount of traffic associated with a TCP/IP service indicated by the message's destination port, or by the relative amount of traffic going though each of the respective network interfaces. In some embodiments, the computers are multi-homed end systems which pick the source address of outgoing messages and their associated socket. In some embodiments, the network interfaces between which messages are distributed are dial-up modems having network-level addresses dynamically allocated to them by the computer to which they are connected. Some systems can automatically connect or disconnect such dial-up connections in response to changes communications demands. In some embodiments of the invention, a multi-homed end system distributes messages addressed to a given destination address between multiple network interfaces for the purpose of load testing." (Killian, Abstract)

By contrast to the foregoing, Aziz, which is concerned with providing secure communication with a relay in a network, discloses:

> "Methods and systems of the present invention include providing a connection between a first computer and a second computer by receiving, at a third computer, information regarding one of the first and second computers to facilitate establishment of a secure connection between the first computer and the second computer, creating a first end-to-end security link between the first computer and third computer, and creating a second end-to-end security link between the second computer and the third computer to establish the secure connection. The first and second computers could be a client and a server on the Internet, and these methods and systems can, for example, increase the possible number of new secure connections to the server. The third computer also permits processing of information transmitted between the client and server in the third computer. For example, the information could be reformatted or used in testing a process of one of the first and second computers." (Aziz, Abstract)

As can clearly be seen, Killian and Aziz, taken alone or in any permissible combination, fail to show, teach or even suggest, a system in which the use of a security token, particularly when that security token is used in creating a socket associated with a first connection, in which the creation of the first connection includes associating the first security token with the first connection. Applicants respectfully submit that the Office Action does not establish the presence of these limitations in Killian and Aziz, taken alone or in any permissible combination.

As an initial matter, Applicants respectfully note that the association between the first security token and the first connection is never addressed in the Office Action. To underscore and more clearly delineate this distinction, Applicants have amended independent claims 107, 120, 131, 140, 165 and 174 to specifically recite this association. Support for this association and related amendments can be found at least, for example, at operation 400 of Figure 4 and p. 11, lines 19 through p. 12, line 15 of the Specification; and other description associated with Figure 4. Thus, no new matter is added thereby.

The Office Action initially states, with regard to claim 107, that:

> "Killian discloses a method comprising: providing a plurality of sockets in a socket table or array, wherein each socket normally represents a connection <u>(i.e., has an associated connection)</u> and each socket has an <u>associated network port</u> and network IP address ..." (Office Action, p. 3; Emphasis supplied)

Applicant respectfully notes that this is said to meet the limitation "... providing a plurality of sockets, wherein each socket has an associated connection and an associated security token (network address). Applicant fails to understand how a socket could separately possess have both a network connection <u>and</u> a network address, given that a network connection includes a network address, by definition. Thus, that being the case, there is no way to successfully draw a parallel between the network address of Killian and a security token, given that Killian's network connection already includes information regarding a network address (i.e., lacking a network address corresponding to the network connection, the network connection cannot exist).

The Office Action goes on to state:

> "Killian discloses <u>the network address</u> is provided by the associated connection ..." (Office Action, p. 4; Emphasis supplied)

These purported teaching of Killian are cited as meeting the limitations of:

"...

providing a plurality of sockets, wherein

each socket has an associated connection and an associated security token,

and

the associated security token is provided by the associated connection;

..."

As an initial matter, Applicants once again note that the Office Action appears to draw a parallel between a network address and security token, a position which has been discussed as being inapposite. Furthermore, a network address is not a security token for the simple fact that a network address does not serve to secure anything, nor is a network address a token in any respect. A security token is one or more units of information that can be used to gain access - for example, a password or verification string.

Furthermore, even if a parallel could successfully be maintained between a network address and a security token (which Applicants maintain is not an appropriate parallel to be drawn from the cited references), nowhere in Killian or Aziz is there shown, taught or suggested an act or apparatus for associating a first security token and a first connection. Aside from the cited references failing to show, teach or suggest a first security token, the actual association of a first security token and a first connection is not shown, taught or suggested by Killian and Aziz, taken alone or in any permissible combination, in any event. As will be appreciated, lacking a teaching of a security token, no such act or apparatus regarding such a feature would be expected to be taught thereby.

Killian is also said to teach "... receiving a first connection and a first security token " – through the citation of the following passages of Killian:

> "When the IP layer receives an outgoing message having a destination IP address equal to that of the Internet provider router, it will use the routing table static entry 132 having that destination address." (Killian, col. 7, line 65, through col. 8, line 2)

and

> "...in such a manner that all the messages associated with a given connection, as defined by the source computational entity identifier, are given the same source network address." (Killian, col. 29, ll. 41-44)

Once again, the Office Action attempts to equate various features disclosed in Killian to the claimed security token. In the above cited sections, instead of the earlier-cited network address, the Office Action attempts to equate first a destination IP address with the claimed security token, then attempts to do so with Killian's source computational entity identifier. Thus, in this regard, the purported parallel between features of Killian and the claimed limitations lead to logical inconsistencies.

In fact, at once, the Office Action attempts to draw a parallel between the claimed security token, and each of a network address, a destination IP address, a source computational entity identifier and a source network address. Quite obviously, all of Killian's cited features cannot be equated to a single limitation (the claimed security token), and, in fact, no such parallels exist with regard to any of the features disclosed by Killian. Applicants are at a loss as to a proper manner in which to respond to such a position. Moreover, did the logical inconsistency in this position not exist under the foregoing reasoning, it would exist for the fact that the purported parallel exists between a source address and a destination address, a position which obviously suffers from lack of internal logical consistency.

Unfortunately, Aziz fails to cure the aforementioned infirmities, as well as the infirmity for which Aziz is cited in the Office Action. First, the logical inconsistencies to which the citations to which Killian fall prey could not be solved by any reference. Moreover, not only is Aziz not cited in regard to the claimed security token, there is no showing, teaching or suggestion In the Office Action (or otherwise), that Aziz could provide such teachings, and in fact, Aziz does not. Crichton, not even cited against these claims, would also provide a fruitless avenue, failing to show, teach or suggest anything even remotely comparable to the claimed security token, even if such features were taken only by themselves (which Applicants maintain is inapposite, given that all the features are cited against the same limitation).

The Office Action thus fails to establish the presence of the foregoing limitations in Killian and Aziz, taken alone or in permissible combination. As will be appreciated, the Office Action bears the burden of supporting a case of obviousness, including whether the prior art references teach or suggest all of the claim limitations. *See* MPEP 706.02(j). For at least the foregoing reasons, neither Killian nor Aziz, alone or in combination (even in view of Crichton), shows, teaches or suggests such limitations.

In addition, Applicants also respectfully submit that the Examiner has not satisfied the burden of factually supporting the alleged motivation to combine the two references. The Examiner's duty may not be satisfied by engaging impermissible hindsight; any conclusion of obviousness must be reached on the basis of facts gleaned from the references. The Examiner must therefore provide evidence to suggest the combination and "[b]road conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" *See In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). While the Office Action cites portions of Aziz for its purported teachings with regard to providing secure communication with a relay in a network, Applicants respectfully submit that no portion or portions of either reference is cited with regard to any motivation provided by either reference for combination with the other, nor any pertinence of any such portion (were such to exist, a position Applicants do not concede).

With regard to the motivation to combine the references, then, Applicants respectfully submit that each of Killian and Aziz (as well as Crichton) provide complete, self-contained solutions to the issues each addresses. Thus, as will be appreciated, Killian is directed to a multi-homed end system for increasing computers' network bandwidth. To accomplish this end, a system according to Killian employs network computers having a plurality of network-level interfaces associated with overlapping portions of the network-level address space. By doing so, Killian's network computers distribute outgoing messages to the overlapping portions of the address space between the multiple network interfaces associated with those overlapping portions. As will be appreciated, then, Killian already provides for communication between computers on a network, in a situation in which multiple computers are to receive the same outgoing messages.

By contrast, Aziz is directed to providing secure communication with a relay in a network. Aziz accomplishes this by providing a connection between a first computer and a second computer by receiving, at a third computer, information regarding one of the first and second computers to facilitate establishment of a secure connection between the first computer and the second computer. As will be appreciated, then, Aziz already provides for communication between computers on a network., providing secure communication with a relay in a network by between a first computer and a second computer by receiving, at a third computer, information regarding one of the first and second computers to facilitate establishment of a secure connection between the first computer and the second computer.

Applicants are once again at a loss as to how the network systems of Killian and Aziz find any need of each other's capabilities (at least, without the recognition of the problem and solution thereto, provided by the disclosure of the claimed invention). The Office Action, however, states that such lies in a desire to "create two separate connections at each end system to provide an application-specific authentication and link them to a secure connection between two end systems when messages are exchanged between computers." (Office Action, p. 5) First, Applicants fail to discern any such need demonstrated by either reference. Certainly, the Office Action fails to demonstrate the existence of such motivation in either reference, given that neither is cited in any way for such a proposition. Furthermore, Applicants are unable to discern any difference between what the Office Action characterizes as the resulting system and the network system of Aziz. Finally, Applicants fail to see, even if this statement were true, how such a system would make obvious the claimed invention.

Further, the Office action fails to establish that such a combination of the teachings of these references would meet with success, as is also required. Applicants maintain that Killian and Aziz, in any permissible combination, fail to teach the claimed invention. At best, although Applicants maintain that one of skill in the art would not find such teachings in either reference (and again, aside from using the present Specification as a blueprint, would be forced into undue experimentation to arrive at such a solution), such a combination would at best provide a multi-homed network system in which one or more such connections could be sent via a network connection that provides secure communication with a relay in a network. Regardless, such a system, even if such a combination were shown to be possible, would fail to make obvious the claimed invention, which involves the use of security tokens in the creation of a socket as a result of the receipt of a first connection and a security token.

For these reasons, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness of amended independent claims 107, 120, 131, 140, 165 and 174, and all claims dependent upon them, and that they are in condition for allowance. Applicants therefore request the Examiner's reconsideration of the rejections to those claims.

Further, claims 116-119 are said to be unpatentable over Killian in view of Aziz, in further view of Crichton. To reiterate, Applicants respectfully traverse this rejection, for the foregoing reasons, as well as those now presented.

Claim 116, for example, recites:

116. The method of Claim 115, wherein
the first connection is created by a protocol daemon.

Applicants agree that this limitation is not taught by Killian and Aziz, taken alone or in any permissible combination. However, Applicants respectfully disagree that neither this, nor any other infirmity, is cured by the addition Crichton, or even that Crichton can be successfully combined with Killian and Aziz.

By contrast to the foregoing, Crichton, which is concerned with lightweight secure communication tunneling over the internet, discloses:

> "A lightweight secure tunneling protocol or LSTP permits communicating across one or more firewalls by using a middle server or proxy. Three proxies are used to establish an end-to-end connection that navigates through the firewalls. In a typical configuration, a server is behind a first firewall and a client behind a second firewall are interconnected by an untrusted network (e.g., the Internet) between the firewalls. A first inside firewall SOCKS-aware server-side end proxy

connects to the server inside the first firewall. A second inside firewall SOCKS-aware client-side end proxy is connected to by the client inside the second firewall. Both server-side and client-side end proxies can address a third proxy (called a middle proxy) outside the two firewalls. The middle proxy is usually started first, as the other two end proxies (server and client) will initiate the connection to the middle proxy some time after they are started. Since the middle proxy is mutually addressable by both inside proxies, a complete end-to-end connection between the server and client is established. It is the use of one or more middle proxies together with the LSTP that establishes the secure communications link or tunnel across multiple firewalls." (Crichton, Abstract)

Applicants do not see that Crichton provides any meaningful supplement to Killian or Aziz, and, in fact, fails to inform any argument as to the purported obviousness of the claims in question. The use of a virtual private network (VPN) through a firewall using known techniques is not material to either the purported combination of Killian and Aziz, or the claimed invention. Applicants fail to appreciate how Crichton differs meaningfully from Aziz, and so are left to question why one of skill in the art would find any reason to look to what is fundamentally a cumulative source of information to Aziz.

For these reasons, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness of claims X and Y, and all claims dependent upon them, and that they are in condition for allowance. Applicants therefore request the Examiner's reconsideration of the rejections to those claims.

CONCLUSION

In view of the amendments and remarks set forth herein, the application and the claims therein are believed to be in condition for allowance without any further examination and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is invited to telephone the undersigned at 512-439-5090.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Mail Stop Amendment, COMMISSIONER FOR PATENTS, P. O. Box 1450, Alexandria, VA 22313-1450, on July 27, 2007.

	7/27/07
Attorney for Applicants	Date of Signature

Respectfully submitted,

Sam G. Campbell III
Attorney for Applicants
Reg. No. 42,381
(512) 439-5084 [Phone]
(512) 439-5099 [Fax]